



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/809,532

03/26/2004

Akira Yaegashi

SON-2960

7528

23353 7590 06/19/2007
RADER FISHMAN & GRAUER PLLC
LION BUILDING
1233 20TH STREET N.W., SUITE 501
WASHINGTON, DC 20036

EXAMINER

CUTLER, ALBERT H

ART UNIT

PAPER NUMBER

2622

MAIL DATE

DELIVERY MODE

06/19/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/809,532	Applicant(s) YAEGASHI, AKIRA	
	Examiner Albert H. Cutler	Art Unit 2622	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is responsive to application 10/809,532 filed on March 26, 2004. Claims 1-17 are pending in the application and have been examined by the examiner.

Information Disclosure Statement

2. The Information Disclosure Statement (IDS) mailed on April 23, 2007 was received and has been considered by the examiner.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 17 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter as follows. Claim 17 defines a program embodying functional descriptive material. However, the claim does not define a computer-readable medium or memory and is thus non-statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-readable medium

Art Unit: 2622

it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of the technology permits the function of the descriptive material to be realized" – Guidelines Annex IV). That is, the scope of the presently claimed 17 can range from a paper on which the program is written to a program simply contemplated and memorized by a person. The examiner suggests amending the claim to embody the program on "computer-readable medium" or equivalent in order to make the claim statutory. Any amendment to the claim should be commensurate with its corresponding disclosure.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 5-7 are rejected under 35 U.S.C. 102(b) as being anticipated by Wakao et al.(US 2002/0060736).

Consider claim 5, Wakao et al. teach:

An image pickup apparatus(10, figure 1, figure 12) used in an image transmission system(figure 12) for transmitting an image via a network(paragraph 0041), said image pickup apparatus(10) comprising:

Art Unit: 2622

a recording unit(17) for recording a unique identifying number(paragraph 0043);
an encrypting unit for encrypting a picked-up image(paragraphs 0043, 0053,
0058; 0067); and

a communicating unit for transmitting said encrypted image to said network(The encrypted image data is sent from the image generation device(10) to the verification data device(20), see figure 12. These two devices can be connected via a LAN(i.e. a network), paragraph 0041. An interface unit(16) and program memory(17) are used to encode and transmit the data, paragraph 0043.).

Consider claim 6, and as applied to claim 5 above, Wakao further teaches:

Said communication unit(16 and 17) includes a receiving unit(17) for receiving an encryption key for encrypting said image from a key generating apparatus(paragraph 0043).

Consider claim 7, and as applied to claim 5 above, Wakao further teaches:

said communicating unit includes a USB port(paragraph 0041).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2622

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claim 1-4, ^{9-12 are} ~~is~~ rejected under 35 U.S.C. 103(a) as being unpatentable over Wakao et al.(US 2002/0060736) in view of Schon et al.(US 7,136,487). y

Consider claim 1, Wakao et al. teach:

An image transmission system for transmitting an image via a network(figures 1-12), said image transmission system comprising:

one or a plurality of image pickup apparatus("Image generation device", 10, figure 1, figure 12, paragraph 0038) each having a unique identifying number("specific ID information", paragraphs 0060, 0062, 0070, 0081, figure 7a) and having an encrypting function for encrypting a picked-up image(paragraphs 0043, 0053, 0058, 0067) for transmission to said network(The encrypted image data is sent from the image generation device(10) to the verification data device(20), see figure 12. These two devices can be connected via a LAN(i.e. a network), paragraph 0041.);

a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for encrypting said image and a decryption key for

Art Unit: 2622

decrypting said encrypted image(An encryption key is generated for each image pickup apparatus(paragraph 0043), and a decryption key is generated for the verification data converting device(paragraph 0045). These keys are stored in the program memory(17) of the image capturing device(10), and the program memory(26) or the verification data converting device(20) respectively. They are contained in tables(figures 7a and 7b) which correlate specific keys with specific imaging devices. See paragraphs 0043-0045.);

a recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other(Table T1, figure 7b, stores decryption keys and identifying numbers of said image pickup apparatus in a ROM or an EEPROM, paragraph 0045.);

an apparatus(20) connected with said recording medium("ROM" or "EEPROM") and having a decrypting function for decrypting said encrypted image using said decryption key(paragraph 0045); and

an authenticating server("Image verification device", 30, figure 12) for authenticating said image pickup apparatus(10) accessible from said viewing apparatus(20)(The image verification device(30) authenticates said image pickup device(10) apparatus by consulting table 7b and finding its identification number, paragraph 0047.).

Wakao et al. further teach a viewing apparatus("display unit", paragraph 0045). However, Wakao et al. do not explicitly teach that the viewing apparatus is used for viewing the image data transmitted via said network by said image pickup apparatus.

Also, although Wakao et al. teach that the decryption key is stored on a ROM or an EEPROM(paragraph 0045), which are commonly embodied on removable memories, Wakao et al. do not explicitly teach that the ROM or EEPROM is removable.

Schon et al. is similar to Wakao et al. in that Schon et al. teach of an image capture device("digital video camera", 41, figure 4) which generates encrypted image data using encryption keys(column 6, line 51 through column 8, line 5). The encrypted image data is similarly sent to a remote device("digital video player", 61, figure 5) where it is decrypted using a key(column 6, line 51 through column 8, line 5).

However, in addition to the teachings of Wakao et al., Schon et al. teach that the viewing apparatus is used for viewing the image data transmitted from said image pickup apparatus(column 4, lines 58-62), and that the decryption key is embodied on a removable recording medium(70, figure 5, column 7, lines 50-54).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to use the viewing apparatus taught by Wakao et al. for viewing the image data as taught by Schon et al., and store the decryption key and image capture device identification number taught by Wakao et al. on a removable storage device as taught by Schon et al. for the benefit of being able to securely view the image data obtained by the pickup device from a remote location(Schon et al. column 4, line 58 through column 5, line 63) and prevent the theft of the decryption key and/or the viewing of the image data by unauthorized individuals, all the while incorporating flexible security intrinsic to both the recordation and playback processes(Schon et al., column 1, line 37 through column 2, line 10.).

Consider claim 2, Wakao et al. teach:

An image transmission system for transmitting an image via a network(figures 1-12), said image transmission system comprising:

one or a plurality of image pickup apparatus("Image generation device", 10, figure 1, figure 12, paragraph 0038) each having a unique identifying number("specific ID information", paragraphs 0060, 0062, 0070, 0081, figure 7a);

a key generating apparatus for encrypting an image picked up by said image pickup apparatus and transmitting the image to said network, and generating a decryption key for decrypting said encrypted image(An encryption key is generated for each image pickup apparatus(paragraph 0043), and a decryption key is generated for the verification data converting device(paragraph 0045). These keys are stored in the program memory(17) of the image capturing device(10), and the program memory(26) or the verification data converting device(20) respectively. They are contained in tables(figures 7a and 7b) which correlate specific keys with specific imaging devices. See paragraphs 0043-0045. See paragraphs 0052-0062 for encryption and transmission of the image data.);

a recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other(Table T1, figure 7b, stores decryption keys and identifying numbers of said image pickup apparatus in a ROM or an EEPROM, paragraph 0045.);

an apparatus(20) connected with said recording medium("ROM" or "EEPROM") and having a decrypting function for decrypting said encrypted image using said decryption key(paragraph 0045); and

an authenticating server("Image verification device", 30, figure 12) for authenticating said image pickup apparatus(10) accessible from said viewing apparatus(20)(The image verification device(30) authenticates said image pickup device(10) apparatus by consulting table 7b and finding its identification number, paragraph 0047.).

Wakao et al. further teach a viewing apparatus("display unit", paragraph 0045). However, Wakao et al. do not explicitly teach that the viewing apparatus is used for viewing the image data transmitted via said network by said image pickup apparatus. Also, although Wakao et al. teach that the decryption key is stored on a ROM or an EEPROM(paragraph 0045), which are commonly embodied on removable memories, Wakao et al. do not explicitly teach that the ROM or EEPROM is removable.

Schon et al. is similar to Wakao et al. in that Schon et al. teach of an image capture device("digital video camera", 41, figure 4) which generates encrypted image data using encryption keys(column 6, line 51 through column 8, line 5). The encrypted image data is similarly sent to a remote device("digital video player", 61, figure 5) where it is decrypted using a key(column 6, line 51 through column 8, line 5).

However, in addition to the teachings of Wakao et al., Schon et al. teach that the viewing apparatus is used for viewing the image data transmitted from said image

Art Unit: 2622

pickup apparatus(column 4, lines 58-62), and that the decryption key is embodied on a removable recording medium(70, figure 5, column 7, lines 50-54).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to use the viewing apparatus taught by Wakao et al. for viewing the image data as taught by Schon et al., and store the decryption key and image capture device identification number taught by Wakao et al. on a removable storage device as taught by Schon et al. for the benefit of being able to securely view the image data obtained by the pickup device from a remote location(Schon et al. column 4, line 58 through column 5, line 63) and prevent the theft of the decryption key and/or the viewing of the image data by unauthorized individuals, all the while incorporating flexible security intrinsic to both the recordation and playback processes(Schon et al., column 1, line 37 through column 2, line 10.).

Consider claim 3, Wakao et al. teach:

An image transmission system for transmitting an image via a network(figures 1-12), said image transmission system comprising:

one or a plurality of image pickup apparatus("Image generation device", 10, figure 1, figure 12, paragraph 0038) each having a unique identifying number("specific ID information", paragraphs 0060, 0062, 0070, 0081, figure 7a);

a transmitting apparatus(interface unit, 16) for encrypting an image picked up by said image pickup apparatus and transmitting the image to said network(paragraph 0043);

a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for encrypting said image and a decryption key for decrypting said encrypted image (An encryption key is generated for each image pickup apparatus (paragraph 0043), and a decryption key is generated for the verification data converting device (paragraph 0045). These keys are stored in the program memory (17) of the image capturing device (10), and the program memory (26) or the verification data converting device (20) respectively. They are contained in tables (figures 7a and 7b) which correlate specific keys with specific imaging devices. See paragraphs 0043-0045.);

a recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other (Table T1, figure 7b, stores decryption keys and identifying numbers of said image pickup apparatus in a ROM or an EEPROM, paragraph 0045.);

an apparatus (20) connected with said recording medium ("ROM" or "EEPROM") and having a decrypting function for decrypting said encrypted image using said decryption key (paragraph 0045); and

an authenticating server ("Image verification device", 30, figure 12) for authenticating said image pickup apparatus (10) accessible from said viewing apparatus (20) (The image verification device (30) authenticates said image pickup device (10) apparatus by consulting table 7b and finding its identification number, paragraph 0047.).

Wakao et al. further teach a viewing apparatus("display unit", paragraph 0045). However, Wakao et al. do not explicitly teach that the viewing apparatus is used for viewing the image data transmitted via said network by said image pickup apparatus. Also, although Wakao et al. teach that the decryption key is stored on a ROM or an EEPROM(paragraph 0045), which are commonly embodied on removable memories, Wakao et al. do not explicitly teach that the ROM or EEPROM is removable.

Schon et al. is similar to Wakao et al. in that Schon et al. teach of an image capture device("digital video camera", 41, figure 4) which generates encrypted image data using encryption keys(column 6, line 51 through column 8, line 5). The encrypted image data is similarly sent to a remote device("digital video player", 61, figure 5) where it is decrypted using a key(column 6, line 51 through column 8, line 5).

However, in addition to the teachings of Wakao et al., Schon et al. teach that the viewing apparatus is used for viewing the image data transmitted from said image pickup apparatus(column 4, lines 58-62), and that the decryption key is embodied on a removable recording medium(70, figure 5, column 7, lines 50-54).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to use the viewing apparatus taught by Wakao et al. for viewing the image data as taught by Schon et al., and store the decryption key and image capture device identification number taught by Wakao et al. on a removable storage device as taught by Schon et al. for the benefit of being able to securely view the image data obtained by the pickup device from a remote location(Schon et al. column 4, line 58 through column 5, line 63) and prevent the theft of the decryption key

Art Unit: 2622

and/or the viewing of the image data by unauthorized individuals, all the while incorporating flexible security intrinsic to both the recordation and playback processes(Schon et al., column 1, line 37 through column 2, line 10.).

Consider claim 4, Wakao et al. teach:

An image transmission system for transmitting an image via a network(figures 1-12), said image transmission system comprising:

one or a plurality of image pickup apparatus("Image generation device", 10, figure 1, figure 12, paragraph 0038) each having a unique identifying number("specific ID information", paragraphs 0060, 0062, 0070, 0081, figure 7a) and having an encrypting function for encrypting a picked-up image(paragraphs 0043, 0053, 0058, 0067) for transmission to said network(The encrypted image data is sent from the image generation device(10) to the verification data device(20), see figure 12. These two devices can be connected via a LAN(i.e. a network), paragraph 0041.);

a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for said image pickup apparatus to encrypt the image and a decryption key(An encryption key is generated for each image pickup apparatus(paragraph 0043), and a decryption key is generated for the verification data converting device(paragraph 0045). These keys are stored in the program memory(17) of the image capturing device(10), and the program memory(26) or the verification data converting device(20) respectively. They are contained in tables(figures 7a and 7b)

Art Unit: 2622

which correlate specific keys with specific imaging devices. See paragraphs 0043-0045.);

a recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other (Table T1, figure 7b, stores decryption keys and identifying numbers of said image pickup apparatus in a ROM or an EEPROM, paragraph 0045.);

an apparatus (20) connected with said recording medium ("ROM" or "EEPROM") and having a decrypting function for decrypting said encrypted image using said decryption key (paragraph 0045); and

Wakao et al. further teach a viewing apparatus ("display unit", paragraph 0045). However, Wakao et al. do not explicitly teach that the viewing apparatus is used for viewing the image data transmitted via said network by said image pickup apparatus. Also, although Wakao et al. teach that the decryption key is stored on a ROM or an EEPROM (paragraph 0045), which are commonly embodied on removable memories, Wakao et al. do not explicitly teach that the ROM or EEPROM is removable.

Schon et al. is similar to Wakao et al. in that Schon et al. teach of an image capture device ("digital video camera", 41, figure 4) which generates encrypted image data using encryption keys (column 6, line 51 through column 8, line 5). The encrypted image data is similarly sent to a remote device ("digital video player", 61, figure 5) where it is decrypted using a key (column 6, line 51 through column 8, line 5).

However, in addition to the teachings of Wakao et al., Schon et al. teach that the viewing apparatus is used for viewing the image data transmitted from said image

Art Unit: 2622

pickup apparatus(column 4, lines 58-62), and that the decryption key is embodied on a removable recording medium(70, figure 5, column 7, lines 50-54).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to use the viewing apparatus taught by Wakao et al. for viewing the image data as taught by Schon et al., and store the decryption key and image capture device identification number taught by Wakao et al. on a removable storage device as taught by Schon et al. for the benefit of being able to securely view the image data obtained by the pickup device from a remote location(Schon et al. column 4, line 58 through column 5, line 63) and prevent the theft of the decryption key and/or the viewing of the image data by unauthorized individuals, all the while incorporating flexible security intrinsic to both the recordation and playback processes(Schon et al., column 1, line 37 through column 2, line 10.).

Consider claim 9, Wakao et al. teach:

An image pickup apparatus unit(10, figure 1, figure 2) comprising:

an image pickup apparatus(10, figure 1, figure 2) having a unique identifying number(paragraph 0043) and having an encrypting function for encrypting a picked-up image for transmission to a network(paragraph 0041-0043); and

a recording medium for recording a decryption key for decrypting the image encrypted by said image pickup apparatus and the identifying number of said image pickup apparatus in association with each other(Table T1, figure 7b, stores decryption

Art Unit: 2622

keys and identifying numbers of said image pickup apparatus in a ROM or an EEPROM, paragraph 0045.).

Also, although Wakao et al. teach that the decryption key is stored on a ROM or an EEPROM(paragraph 0045), which are commonly embodied on removable memories, Wakao et al. do not explicitly teach that the ROM or EEPROM is removable.

Schon et al. is similar to Wakao et al. in that Schon et al. teach of an image capture device("digital video camera", 41, figure 4) which generates encrypted image data using encryption keys(column 6, line 51 through column 8, line 5). The encrypted image data is similarly sent to a remote device("digital video player", 61, figure 5) where it is decrypted using a key(column 6, line 51 through column 8, line 5).

However, in addition to the teachings of Wakao et al., Schon et al. teach that the the decryption key is embodied on a removable recording medium(70, figure 5, column 7, lines 50-54).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to store the decryption key and image capture device identification number taught by Wakao et al. on a removable storage device as taught by Schon et al. for the benefit of preventing the theft of the decryption key and/or the viewing of the image data by unauthorized individuals, all the while incorporating flexible security intrinsic to both the recordation and playback processes(Schon et al., column 1, line 37 through column 2, line 10.).

Consider claim 10, and as applied to claim 9 above, Wakao et al. teach:

said image pickup apparatus receives an encryption key for encrypting said image from a key generating apparatus(See paragraph 0043. An encryption key is received and stored in the program memory(17). The key must come from a key generating apparatus.).

Consider claim 11, and as applied to claim 9 above, Wakao et al. teach of recording a decryption key in memory(paragraph 0045). However, Wakao et al. do not explicitly teach that the decryption key is received by a removable recording medium.

Schon et al. teach that said removable recording medium(70, figure 5) receives the decryption key(73, figure 5) for decrypting said image from a key generating apparatus(Multiple decryption keys are stored(i.e. received by) on the removable memory(column 7, line 55 through column 8, line 5).).

Consider claim 12, and as applied to claim 9 above, Wakao et al. teach said image pickup apparatus is a USB camera(The camera can be connected via USB, paragraph 0041.).

7. Claim 8 is rejected under 35 U.S.C. 103(a) as being obvious over Wakao et al. in view of Monroe(US 7,131,136).

Consider claim 8, and as applied to claim 5 above, Wakao et al. do not explicitly teach the recording unit records an IP address.

Monroe is similar to Wakao et al. in that Monroe teach of cameras(61, 62, 63) which transmit image data over an interface to external devices(see figure 6). Similarly, one of these devices includes a display(72).

However, in addition to the teachings of Wakao et al., Monroe teaches the recording unit records an IP address(The cameras are IP cameras, figure 6, column 33, lines 26-50.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to use an IP camera as taught by Monroe as the image pickup device taught by Wakao et al. because with an IP-based network camera, the network camera immediately digitizes the images and the video stream is ready to be sent over any computer network available, wherein one network cable can easily handle signals from multiple network cameras simultaneously.

8. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wakao et al. in view of Schon et al. as applied to claim 9 above, and further in view of Monroe(US 7,131,136).

Consider claim 13, and as applied to claim 9 above, the combination of Wakao et al. and Schon et al. does not explicitly teach the image pickup apparatus is an IP camera.

Monroe is similar to Wakao et al. in that Monroe teach of cameras(61, 62, 63) which transmit image data over an interface to external devices(see figure 6). Similarly, one of these devices includes a display(72).

However, in addition to the combined teachings of Wakao et al. and Schon et al., Monroe teaches the image pickup apparatus is an IP camera(see figure 6, column 33, lines 26-50).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to use an IP camera as taught by Monroe as the image pickup device taught by the combination of Wakao et al. and Schon et al. because with an IP-based network camera, the network camera immediately digitizes the images and the video stream is ready to be sent over any computer network available, wherein one network cable can easily handle signals from multiple network cameras simultaneously.

9. Claims 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kondoh et al.(US 6,968,058) in view of Schon et al.

Consider claim 14, Kondoh et al. teach:

A key generating apparatus(120, figure 13) for generating an encryption key used for encryption processing in transmitting an image via a network, and a decryption key(column 11, lines 61-66);

wherein said key generating apparatus(120) generates the encryption key for encrypting said image and transmits the encryption key to an image pickup apparatus

Art Unit: 2622

having a unique identifying number and having an encrypting function for encrypting a picked-up image for transmission to the network(column 11, line 55 through column 12, line 65. Kondoh et al. teach that alteration detection data is encrypted and decrypted, which data is stored in the header of the image file, column 5, lines 37-52.); and

said key generating apparatus(120) generates the decryption key for decrypting said encrypted image and transmits the decryption key to a recording medium(203) for recording said decryption key and the identifying number of said image pickup apparatus in association with each other(column 11, line 61 through column 12, line 8, column 12, lines 55-65.).

However, Kondoh et al. do not explicitly teach that the decryption key is recorded on a removable recording medium.

Schon et al. is similar to Kondoh et al. in that Schon et al. teach of an image capture device("digital video camera", 41, figure 4) which generates encrypted image data using encryption keys(column 6, line 51 through column 8, line 5). The encrypted image data is similarly sent to a remote device("digital video player", 61, figure 5) where it is decrypted using a key(column 6, line 51 through column 8, line 5).

However, in addition to the teachings of Kondoh et al., Schon et al. teach that the decryption key is embodied on a removable recording medium(70, figure 5, column 7, lines 50-54).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to store the decryption key and image capture device identification number taught by Wakao et al. on a removable storage device as taught

Art Unit: 2622

by Schon et al. for the benefit of preventing the theft of the decryption key and/or the viewing of the image data by unauthorized individuals, all the while incorporating flexible security intrinsic to both the recordation and playback processes(Schon et al., column 1, line 37 through column 2, line 10.).

Consider claim 15, and as applied to claim 14, Kondoh et al. further teach said key generating apparatus has a linking function for linking said image pickup apparatus to said network(The key generating apparatus links the image pickup apparatus to said network by generating a public key that is stored in a server, which allows a user to access the data anywhere in the world based on the serial number of the camera, column 12, lines 58-65.).

Consider claim 16, Kondoh et al. further teach:

said key generating apparatus has a compressing function for compressing the image picked up by said image pickup apparatus(The generated keys are stored in the header along with compression information, column 4, line 60 through column 5, line 52.).

Consider claim 17, Kondoh et al. teach:

A program for making a computer function as a key generating apparatus(The key generating mechanism(120) generates keys which are stored digitally in memory(column 11, line 56 through column 12 line 65). Because the keys are stored

Art Unit: 2622

on computer readable media, the keys must be generated by a computer, which computer must contain a program for generating said keys.)

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Park(US 2004/0085446) teaches of an image transmission system containing a camera(100) and a viewing apparatus(500), figure 1. The image transmission system of Park also encrypts and decrypts the image data using a key generated from the specific camera number(see figure 2, figure 4, figure 7, figure 8, paragraphs 0068-0070).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Albert H. Cutler whose telephone number is (571)-270-1460. The examiner can normally be reached on Mon-Fri (7:30-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ngoc-Yen Vu can be reached on (571)-272-7320. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2622

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AC

A handwritten signature in black ink, appearing to read 'Lin Ye', with a long horizontal flourish extending to the right.

LIN YE
PRIMARY PATENT EXAMINER